UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/804,832	03/17/2004	Terry D. Perkinson	10041.000100	7133

31894 7590 09/10/2009

OKAMOTO & BENEDICTO, LLP
P.O. BOX 641330
SAN JOSE, CA 95164

EXAMINER	
MCNALLY, MICHAEL S	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
09/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/804,832
Filing Date: March 17, 2004
Appellant(s): PERKINSON, TERRY D.

James K. Okamoto, Reg No. 40,110
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10 July 2009 appealing from the Office action mailed 17 February 2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2005/0034159	OPHIR	10-2005
2003/0147532	HAKKARAINEN	8-2003
5,467,398	PIERCE	11-1995
2004/0253979	BURR	12-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 26-28 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2005/0034159 by *Ophir et al*.

As to **claim 26**, *Ophir* discloses an apparatus for data transfer comprising:

at least one interface module for communicating with data resources (Ophir: 27 – Fig 2A; Page 3, Sec 38 and Page 4, Sec 45; Splitter);

a home wired network interface module for sending and receiving control packets and security packets to and from a wired home network(Ophir: 27 – Fig 2A; Page 3, Sec 38 and Page 4, Sec 45; Splitter);

a wireless network interface module for sending and receiving data packets to and from a wireless home network (*Ophir*: A – Fig 2A; Page 3, Sec 38 and Page 4, Sec 45 ; Antenna); and

a processing unit for encapsulating data packets, de-encapsulating said data packets, processing said security packets, processing said control packets, detecting a second processing unit on both said home wired network and said wireless network and delivering said data packets on said wireless network interface module to said second processing unit (Ophir: 20 – Fig 2A; Page 3, Sec 38 and Page 4, Sec 45; STB/DVD/PVR processor).

As to **claim 27**, *Ophir* further discloses wherein said data resources are selected from the group comprising internet, cable, telephone, digital versatile disc, personal video recorder, personal computer and video camera (*Ophir*: Page 1, Sec 19).

As to **claim 28**, *Ophir* further discloses wherein said apparatus is integrated within home entertainment and computing equipment (*Ophir:* Fig 2a, Page 4, Sec 45).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-5, 7-9 and 13-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2005/0034159 by *Ophir et al.* in view of U.S. Patent Application Publication No. 2003/0147532 by *Hakkarainen et al.*

As to **claim 1**, *Ophir* discloses an apparatus for data transfer comprising:

a plurality of nodes that are configured to be communicatively interconnected by both a first network which is a wireless home network and a second network which is a wired home network (*Ophir*: Fig 1; Page 3, Sec 32-37; Appliances in a home are connected to both a wireless 802.11 network and the home coaxial cable network),

wherein secured data is transferred between at least two nodes of said plurality of nodes on said first network(*Ophir*: Page 5, Sec 50; Protected cable video transmitted over 802.11 network, DOCSIS packets transmitted over coax lines).

Ophir does not expressly disclose wherein secured data is transferred between at least two nodes of said plurality of nodes on said first network only if said at least two nodes also exist on said second network.

Hakkarainen discloses wherein secured data is transferred between at least two nodes of said plurality of nodes on said first network only if said at least two nodes also exist on said second network (*Hakkarainen*: Figs 1 and 6; Pages 1-2, Sec 14-19 and Pages 3-4, Sec 25-37; In order for the service provider to transmit data on the broadcast channel, it is required that the client be connected to the service provider on the interaction channel).

Ophir and *Hakkarainen* are analogous art because they are from the common area of data broadcast and delivery services.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine the multi-channel scheme of *Hakkarainen* with the hybrid network of *Ophir*. The rationale would have been to securely provide decryption information to clients (*Hakkarainen*: Page 1, Sec 15)

As to **claim 2**, the modified *Ophir/Hakkarainen* reference further discloses wherein unsecured data is freely transferred between said at least two nodes on said first network (*Ophir*: Page 5, Sec 47).

As to **claim 3**, the modified *Ophir/Hakkarainen* reference further discloses wherein unsecured data is freely transferred between said at least two nodes on said second network (*Ophir*: Page 5, Sec 48).

As to **claim 4**, the modified *Ophir/Hakkarainen* reference further discloses wherein said at least two nodes exist on said second network for the entire period of said data transfer across said first network (*Hakkarainen*: Figs 1 and 6; Pages 1-2, Sec 14-19 and Pages 3-4, Sec 25-37).

As to **claim 5**, the modified *Ophir/Hakkarainen* reference further discloses further including security negotiation for use of said first network wherein said security negotiation data is transferred between said at least two nodes only over said second network (*Hakkarainen*: Figs 1 and 6; Pages 1-2, Sec 14-19 and Pages 3-4, Sec 25-37).

As to **claim 7**, the modified *Ophir/Hakkarainen* reference further discloses wherein said second network is a home electrical wiring network (Ophir: Page 1, Sec 7).

As to **claim 8**, the modified *Ophir/Hakkarainen* reference further discloses further including at least one interface module for communicating with data resources (*Ophir*: 15a – Fig 1; Page 3, Sec 34; Home splitter).

As to **claim 9**, the modified *Ophir/Hakkarainen* reference further discloses wherein said security negotiation further includes at least one authentication key (*Hakkarainen*: Figs 1 and 6; Pages 1-2, Sec 14-19 and Pages 3-4, Sec 25-37).

As to **claim 13**, the modified *Ophir/Hakkarainen* reference further discloses wherein said authentication key is established by one of the group consisting of the

manufacturer, the service provider, the end user and a predetermined algorithm (*Hakkarainen*: Figs 1 and 6; Pages 1-2, Sec 14-19 and Pages 3-4, Sec 25-37).

As to **claim 14**, the modified *Ophir/Hakkarainen* reference further discloses wherein said wired home network has predetermined physical boundaries (*Ophir*: Fig 1, 4; Cable network for a home is bounded by the four walls of the home).

As to **claim 15**, the modified *Ophir/Hakkarainen* reference further discloses wherein said wired home network is selected from the group comprising facility electrical wiring network, a home PNA telephone wiring network, a standard wired Ethernet network, and a coaxial cable network (*Ophir*: Page 3, Sec 34, Coaxial cable CX).

As to **claim 16**, the modified *Ophir/Hakkarainen* reference further discloses wherein said wired home network further includes predetermined physical access points (*Ophir:* Page 1, Sec 7).

As to **claim 17**, the modified *Ophir/Hakkarainen* reference further discloses wherein said physical access points include at least one selected from the group consisting of electrical outlets, phone jacks, and Ethernet jacks (*Ophir:* Page 1, Sec 7).

Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2005/0034159 by *Ophir et al.* in view of U.S. Patent Application Publication No. 2003/0147532 by *Hakkarainen et al* further in view of U.S. Patent No. 5,467,398 to *Pierce et al.*

As to **claim 11**, the modified *Ophir/Hakkarainen* reference discloses all recited elements of claim 9 from which claim 11 depends.

The modified reference does not expressly disclose wherein said authentication key is periodically changed.

Pierce discloses wherein said authentication key is periodically changed (*Pierce*: Fig 2-3; Col 4 -5, Lines 55-49).

The modified reference and *Pierce* are analogous art because they are from the common area of network communications.

At the time of invention, it would have been obvious to a person of ordinary skill in the art to periodically change an authentication key. The rationale would have been to reduce the potential to have the key cloned (*Pierce*: Col 5, Lines 46-49).

As to **claim 12**, the modified *Ophir/Hakkarainen/Pierce* reference further discloses wherein said authentication key is randomly changed (*Pierce*: Fig 2-3; Col 4 - 5, Lines 55-49).

Claims 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0253979 to *Burr*. in view of U.S. Patent Application Publication No. 2005/0034159 by *Ophir et al*.

As to **claim 18,** *Burr* discloses A method for data transfer between at least two nodes of a plurality of nodes over a first network using a second network for authentication (*Burr*: Fig 1; Page 3, Sec 27; Network 190 used to authenticate data sent over data 180), the method comprising:

authenticating a relationship between said at least two nodes on said second network (*Burr*: 320 - Fig 3; Page 4, Sec 34);

transferring data between said at least two nodes on said first network (*Burr*: 360 – Fig 3; Page 4, Sec 37);

re-authenticating a relationship between at least two nodes on said second network (*Burr*: 340 – Fig 3; Page 4, Sec 37); and

de-authenticating a relationship between at least two nodes (*Burr*: 370 – Fig 3; Page 4, Sec 39).

Burr does not expressly disclose data transfer between at least two nodes of a plurality of nodes within a home.

Ophir discloses data transfer between at least two nodes of a plurality of nodes within a home (*Ophir*: Fig 1; Page 3, Sec 32-37).

Burr and *Ophir* are analogous art because they are from common area of network communications.

At the time of invention, it would have been obvious to a person of ordinary skill in the art to transfer data within two or nodes within a home The rationale would have been to share content among in-home appliances (*Ophir*: Page 5, Sec 48).

As to **claim 19**, the modified *Burr/Ophir* reference further discloses wherein said step of authenticating comprises determining whether said at least two nodes within the home (*Ophir*: Fig 1; Page 3, Sec 32-37) exist on both said first network and said second network (*Burr*: Page 3, Sec 27).

As to **claim 20**, the modified *Burr/Ophir* reference further discloses wherein said step of authenticating said relationship between at least two nodes of said plurality of

nodes is repeated periodically on said second network throughout the duration of said data transfer (*Burr*: Page 4, Sec 36).

As to **claim 21**, the modified *Burr/Ophir* reference further discloses wherein said step of de-authenticating said relationship between at least two nodes is conducted on said second network (*Burr*: 370 – Fig 3; Page 4, Sec 39).

As to **claim 22**, the modified *Burr/Ophir* reference further discloses wherein said first network is a wireless home network and said second network is a wired home network (*Ophir*: Fig 1; Page 3, Sec 32-37; Appliances in a home are connected to both a wireless 802.11 network and the home coaxial cable network).

As to **claim 23**, the modified *Burr/Ophir* reference discloses an apparatus for data transfer between at least two nodes of a plurality of nodes within a home (*Ophir*: Fig 1; Page 3, Sec 32-37) over a first network using a second network for authentication (*Burr*: Fig 1; Page 3, Sec 27; Network 190 used to authenticate data sent over data 180), the apparatus comprising:

means for authenticating a relationship between said at least two nodes within the home on said second network (*Burr*: 320 - Fig 3; Page 4, Sec 34);

means for transferring data between said at least two nodes within the home on said first network (*Burr*: 360 – Fig 3; Page 4, Sec 37);

means for re-authenticating a relationship between said at least two nodes within the home on said second network (*Burr*: 340 – Fig 3; Page 4, Sec 37); and

means for de-authenticating a relationship between said at least two nodes within the home on said second network (*Burr*: 370 – Fig 3; Page 4, Sec 39).

As to **claim 24**, the modified *Burr/Ophir* reference further discloses wherein said step of authenticating comprises determining whether said at least two nodes exist on both said first network and said second network (*Burr*: Page 3, Sec 27).

As to **claim 25**, the modified *Burr/Ophir* reference further discloses wherein said first network is a wireless home network and said second network is a wired home network *Ophir*: Fig 1; Page 3, Sec 32-37; Appliances in a home are connected to both a wireless 802.11 network and the home coaxial cable network).

(10) Response to Argument

With respect to claim 1, Appellant argues that "**claim 1 expressly recites, "wherein secured data is transferred between at least two nodes of said plurality of nodes on said first network only if said two nodes also exist on said second network**" and that Hakkarainen fails to disclose this limitation because Hakkarainen "**does not check whether the connection to the client via the bidirectional link is maintained in order to continue the data transfer and actually reconnects to the client via the bi-directional channel if a new seed and synchronization information is needed**."

This argument is unpersuasive. the language of claim 1 requires that there be a plurality of nodes, that the plurality of nodes are interconnected by two networks, one wired and one wireless, and that secured data be exchanged between two nodes on the first network only if the same two nodes "exist" on the second network. Hakkarainen is

relied upon to disclose the feature "**wherein secured data is transferred between at least two nodes of said plurality of nodes on said first network only if said two nodes also exist on said second network.**" As disclosed in the rejection of claim 1, as presented above, Hakkarainen discloses a plurality of nodes (service Provider 10 and Client 12, Figure 1) that are connected by a first network (Broadcast Channel 16, Figure 1; also referred to as the unidirectional channel) and a second network (Interaction Channel 14, Figure 1; also referred to as the bidirectional channel), and that secured data is transferred between the two nodes on the first network only if said at least two nodes also exist on said second network (Pages 1-2, Paragraphs 15-17; "Service provider 10 encrypts the services being broadcast on the unidirectional channel 16 using encryption information...The service provider 10 uses the bidirectional channel 14 to receive service requests and authenticate clients 12....Service provider 10 also uses the bidirectional channel to transmit initial decryption information ...needed to begin decrypting a service.") Thus, in order for the client to be able to decrypt data sent over the broadcast channel, it must necessarily exist on the network created by the interaction channel to receive, at the very least, the initial decryption information. This at the very least meets the claimed limitation of **"wherein secured data is transferred between at least two nodes of said plurality of nodes on said first network only if said two nodes also exist on said second network**". Appellant has not claimed the feature of "**check(ing) whether the connection to the client via the bidirectional link is maintained in order to continue the data transfer,"** and as such, arguments directed to this feature, which is not inherent in Appellants claim, are not persuasive as

they are directed to unclaimed features or limitations. Furthermore, Appellants assertion that the invention of Hakkarainen "**reconnects to the client via the bi-directional channel if a new seed and synchronization information is needed**" is not persuasive as the language of claim 1 does not require that the nodes on the second network be continuously active (as implied by Appellants argument), but only that they "exist" on the second network. The fact that the communication over the interaction channel is a necessary precondition for successful broadcast and decryption over the broadcast channel clearly shows that the two nodes "exist" on the second network (the interaction channel) and that secured (encrypted) information can only be transferred across the first network (the broadcast channel) if the nodes have such a connection and exist on the second network.

With respect to claim 4, Appellant argues that claim 4 further recites "**The apparatus of claim 1 wherein said at least two nodes exist on said second network for the entire period of said data transfer across said first network**" and "**that per the cited disclosure of Hakkarainen, the bidirectional channel 14 is used to merely authenticate the client prior to transmitting data via the unidirectional channel 16. However, the service provider (i) does not check whether the connection to the client via the bidirectional channel is maintained in order to continue the data transfer and (ii) actually reconnects to the client via the bidirectional channel if a new seed and synchronization information is needed.**"

This argument is unpersuasive. The language of claim 4 requires that the nodes "exist" on the second network for the entire period of the data transfer across the first

network. "Existing" on a network is not defined or further limited in the claim or in Appellants specification, and Appellants arguments imply that to "exist" on a network means that the nodes on the network must be actively exchanging information. This limitation has not been claimed, and on that basis it is unpersuasive. Furthermore, such an argument lacks a factual basis. Take for example telephones with assigned telephone numbers that are connected to the public switched telephone network (hereinafter PSTN). This example is used in part because the PSTN is one possible embodiment of the bidirectional channel as disclosed by Hakkarainen on Page 1, Paragraph 16. A device that has an assigned telephone number and that is connected by appropriate means to the network "exists" on that network, regardless of whether or not it is actively communicating with any other node on the PSTN at a point in time. Any other interpretation of "exists" in this context simply makes no sense – Appellant is effectively arguing that a device that is not actively communicating does not exist on a network. The same logic applies to Internet Protocol (IP) networks as well. Nodes on an IP network have addresses that are used to route information to the node and identify the source of information from the node. If a computer connected to and IP network is not actively exchanging packets with some other node, it simply cannot be said that it doesn't "exist" on the IP network. Only if it is incapable of communication with any other node on the IP network can it be said that a node does not "exist" on the network - for example, a computer with no IP address does not "exist" on the IP network. Thus, Appellant's contention that "**the service provider (i) does not check whether the connection to the client via the bidirectional channel is maintained in**

order to continue the data transfer" is unpersuasive as directed to an unclaimed limitation and that "**reconnect(ing) to the client via the bidirectional channel if a new seed and synchronization information is needed"** is unpersuasive as it is not determinative of whether the node "exist" on the network for the entire period of the data transfer, as Examiner has clearly shown that "existing" on a network does not imply active continuous communication between nodes as alleged by Appellant.

With respect to claims 11 and 12, Appellant argues that Pierce fails to cure the deficiencies of Ophir in view of Hakkarainen as described in the arguments presented with respect to claims 1 and 4. Examiner has addressed Appellants arguments with respect to claims 1 and 4 above, and believes that no further explanation is needed with respect to claims 11 and 12.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Michael S McNally/

Examiner, Art Unit 2436

Conferees:

/Farid Homayounmehr/

AU: 2439

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436